Triple Layer Security to Data in Cloud

R.Kalaivani

Asst Professor, Dept of CS,MSN Pioneer Meenakshi Women's College, Poovanthi,Tamil Nadu

***Abstract-- Cloud* computing is the buzz word in today's IT world. It is used to store enormous amount of data and able to access these data at anytime, anywhere on demand. There are many Cloud Service Providers (CSP) such as Google, Microsoft, IBM, Oracle Corporation, Amazon Web Services, etc. which provide cloud services to users. Since data in cloud might be stored in data servers throughout the world, data stored in cloud is prone to be hacked. Also it involves sending data over internet, security breach needs to be monitored and controlled. In this paper I introduce a new hybrid algorithm which is a combination of three algorithms namely RSA, AES and Steganography .It will provide security to the data while being uploaded or downloaded from cloud.**

***Keywords*-- Cloud Computing, Security, RSA, AES and Steganography**

I. Introduction

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., servers, storage, networks, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[1]. Essential Cloud Characteristics can be listed as

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service.

The concept of cloud computing is associated closely with Infrastructure as a Services (IaaS), Platform as a Services (PaaS), Software as a Services (SaaS) all of which means a service oriented architecture .These provides the first benefit of the cloud computing (i.e.) it reduce cost of hardware that cloud have been used at end user. As there is no need to store data at end user's because it is already at some other location. So instead of buying the whole infrastructure required to run the process and save bulk of data you are just renting the assets according to your requirement [2].

The following figure illustrates the advantage and disadvantages of cloud computing.

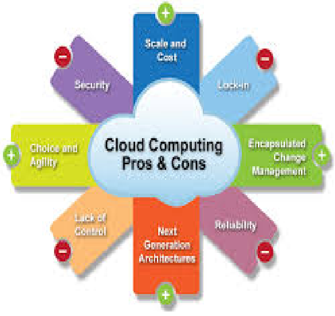
Scale and Cost
Lock-in
Security
Choice and Agility
Cloud Computing Pros & Cons
Encapsulated Change Management
Lack of Control
Next Generation Architectures
Reliability

Figure 1 – Advantages & Disadvantages of Cloud Computing

In this paper I focus on how to resolve one of the disadvantage -security, the security of data to be stored in cloud computing.

II. Security In Cloud Computing

The major problem we are facing in cloud computing is Security. To ensure security in data stored in cloud, there are so many risk associated with the cloud network like data can be hacked by an unauthorized person. Data can be changed by third party while transferring the data . In this paper I present the triple layer of security to the data, in which first layer is to encode data using DSA (Digital Signature Algorithm). In the second layer, the data is encrypted using Advance Encryption Standard Algorithm. AS a third layer, Encrypted data is going to be hidden in digital image using the Steganography method.

III. Methods Of Security Provided To Data

A.RSA Algorithm

RSA:Very common and the first, PKC implementation, which is named for the three MIT mathematicians Ronald Rivest, Adi Shamir, and Leonard Adleman who developed it. RSA today is used in several software products and it can be used for digital signatures, key exchange, or encryption of small blocks of data. RSA uses a variable size key and a variable size encryption block. The key -pair is derived from a very large number, n, that is the product of two prime numbers chosen according to special rules; these primes may be 100 or more digits in length each, yielding an n with roughly twice as many digits as the prime factors. The public key information includes n and a derivative of one of the factors of n; an attacker cannot determine the prime factors of n(and, therefore, the private key) from this information alone and that is what makes the RSA algorithm so secure.[3]

```
Algorithm
Key Generation: KeyGen
(p, q)
Input: Two large primes –p, q
Compute n = p . q
φ (n) = (p -1)(q -1)
Choose e such that gcd(e, φ (n)) = 1
Determine d such that e . d ≡ 1 mod φ (n)
Key:
public key = (e, n) and secret key= (d, n)
Encryption:
c = me mod n where c is the cipher text and m is the plain text.
```

RSA has a multiplicative homomorphic property i.e., it is possible to find the product of the plain text by multiplying the cipher texts. The result of the operation will be the cipher text of the product.

Given ci = E(mi) = mi e mod n,

Then (c1. c2) mod n = (m1. m2) e mod n [3]

B.AES

AES: (Advanced Encryption Standard), is the new encryption standard recommended by NIST to replace DES. Brute force attack is the only effective attack known against it, in which the attacker tries to test all the characters combinations to unlock the encryption. Both AES and DES are block ciphers. It has variable key length of 128, 192, or 256 bits; default 256. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES Encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications. [4]

Its algorithm is as follows:

1. Key Expansion
2. Initial Round
3. Add Round Key
4. Rounds
5. Sub Bytes -a non-linear substitution step where each byte is replaced with another according to a lookup table.
6. Shift Rows -a transposition step where each row of the state is shifted cyclically a certain number of steps.
7. Mix Columns -a mixing operation which operates on the columns of the state, combining the four bytes in each column
8. Add Round Key -each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.
9. Final Round (no Mix Columns)
10. Sub Bytes
11. Shift Rows
12. Add Round Key [5]

C.Steganography

Steganography is be a Greek work which implies the covered writing. Steganography is associate art of hiding data in an exceedingly covered media (image, audio, video, text). The lined media is chosen in such a fashion that it's capability to cover the information and hardiness that has quality to the stego image. As within the future years the requirement of knowledge activity, copyright protection, and confidentiality will increase, steganography plays a crucial role in this field as a result of its some distinctive options. In Steganography thus not only emphasize on the art of hiding information but also the art and science of hiding the communication that take place [6]. First applications of Steganography were documented by Herodotus, a Greek historian. During the century, the methods of using invisible inks were extremely popular [7]. During the World War II where people used ink for writing hidden messages, this was true [8]. The mixture will turn darker and the written message becomes visible upon heating. After some time, the Germans introduced the microdot technique where microdots are considered as photographs as small as a printed period, but with a clear format of a typewritten page .They were included in a letter or an envelope, and because of their tiny sizes, they could be indiscernible. Microdots were also hidden in body parts including nostrils, ears, or under fingernails [6].The military and several governmental agencies are looking into steganography for their own secret transmissions of information. The following list explains the different types of Steganography.

i) Text Steganography:It consists of concealing data within the text files. In this methodology, the key data Is hidden behind each ordinal letter of each words of text message. Numbers of ways are accessible for concealing knowledge in document. These ways are

i)Format based mostly methodology;
ii)Random and statistical Method;
iii)Linguistics Method.

2) Image Steganography:
It concealing the information by taking the duvet object as image is referred as image steganography. In image steganography element intensities are accustomed hide the info. In digital steganography, pictures are widely used cover source as a result of there is range of bits presents in digital illustration of a picture.

3) Audio Steganography:
It involves concealing data in audio files. This methodology hides the info in WAV,
AUand MP3 sound files. There are completely different ways of audio steganography. These ways are
i) Low Bit encryption
ii) Phase coding
iii) Spread Spectrum.

4) Video Steganography:
It's a method of concealing any kind of files or data into digital video format. In this case video (combination of pictures) is employed as carrier for concealing the info. Typically separate trigonometric function transform (DCT) alter the values (e.g., 8.667 to 9) that is employed to cover the information in every of the images within the video, that is unnoticeable by the human eye. H.264, Mp4, MPEG, AVI are the formats used by video steganography.[9]

IV.OVERALL DESIGN OF PROPOSED WORK

In our proposed work we provide security by implementing three algorithms RSA, AES and steganography together to cloud network. To implement these three algorithms I use Asp.net as a platform.

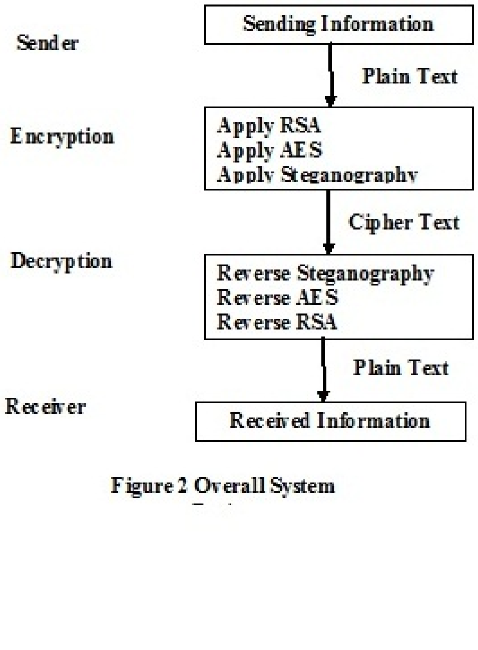

Figure 2 Overall System

In my proposed system for encryption, first I apply RSA for authentication of data. Then I apply AES algorithm for encryption and then hiding data within image file for provide maximum security to the data. Receiver can get original plain text by reversing the steganography, AES and RSA.

V.Conclusion And Future Work

In this paper I implements RSA, AES and Steganography to provide maximum security in cloud computing. By implementing these three algorithms I try to provide authenticity, security and data integrity to that data. We find that the Time complexity is high because it is a one by one process but in future this time complexity could be reduced. I try to improve the time complexity by using other security algorithms.

References

1. http://www.wikipedia.org/cloud_computing
2. Vanya Diwan, Shubhra Malhotra,Rachna Jain,Bharati ,, "Cloud Security Solutions: Comparison among Various Cryptographic Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering Volume 4,, Issue 4,April 2014 ,ISSN: 2277 128X
3. Charanjeet Kaur,Gurjit Singh Bhathal, "Data Security Algorithms In Cloud Computing: A Review", International Journal For Technological Research In Engineering, Volume 2, Issue 5, January-2015,ISSN (Online): 2347 -4718
4. Garima Saini, Naveen Sharma, "Triple Security of Data in Cloud Computing ", International Journal of Computer Science and Information Technologies, Vol. 5 (4), 2014, 5825-5827, ISSN: 0975-9646
5. Gurpreet Singh, Supriya Kinger, "Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security", International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.
5. D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009.
6. K.S.Wagh, Swapnil Chaudhari, and Anita Deshmukh at al., "Data Security in Cloud Computing", In proceeding of International Journal of Current Engineering and Technology, 2014
7. M.K.Sarkar and Trijit Chatterjee, "Enhancing Data Storage Security in Cloud Computing Through Steganography", ACEEE Int. J.on Network Security, Vol. 5, No. 1, Jan 2014.
8. R.Bala Chandar, M.S.Kavitha and K.Seenivasan, "A proficient model for high end security in cloud ccomputing", ICTACT journal on soft computing, Vol. 04, issue: 02, Jan 2014.
9. Alok Ranjan,Mansi Bhonsle," A Review of Privacy Protection of Cloud Storage andSteganography Techniques ",International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 | Impact Factor (2014): 5.611